IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. At a general level, my analysis of Georgia's new election equipment has revealed that, despite the addition of a paper trail, individual Georgia voters who use BMDs face security risks that are *worse* than the risks they faced when voting on DREs.

3. Paper ballots and risk-limiting audits are often thought of as the "gold standard" for election security, because, when applied in certain ways, they can detect

and correct any outcome-changing cyberattack on the election technology. Yet, in Georgia, a series of missteps in the design and implementation of the election system have rendered these critical protections ineffective. These missteps and other security defects expose Georgia voters to severe risks that their individual votes will not be counted accurately, if at all.

4. Georgia requires nearly all in-person voters to use BMDs. These voters' ballots are counted based on barcodes, which voters cannot read or verify. While the ballots also contain human-readable text, with rare exceptions this text is completely ignored during counting. (State rules call for using a risk-limiting audit to confirm that the election outcome matches the human-readable portion of the ballots in only a single contest every two years, and even in the event of a candidate-initiated recount, the election result is typically determined from the barcodes.) As a result, an attacker who could infiltrate the BMDs and manipulate the barcodes could change votes for individual voters such as Curling Plaintiffs without detection, as if the paper trail did not exist. This could be done in a manner that does or does not affect the election outcome, depending on the manner of the attack—but the result nonetheless would be the alteration or loss of personal votes for the individual voters affected.

5. The risk of such an attack depends on the feasibility of hacking an individual BMD to manipulate votes without detection, such as by altering the

corresponding barcodes. Where the objective of the attack also is to alter an election outcome, the risk additionally would depend on the likelihood that attackers can compromise *sufficiently many* votes (across multiple BMDs, depending on the election) to accomplish that objective. The Plaintiffs have asked me to perform technical assessments of these risks.

6. [redacted]

7. [redacted]

[1] Halderman Decl. (Dec. 16, 2019), Dkt. 682 at ¶ 8.

[redacted].[2]

8. [redacted]

9. [redacted]

[2] [redacted] Dckt. 906 at 31:12-18.

[redacted]

10. [redacted]

[redacted]

[3] *See*: Secretary of State's Office, "Secretary Raffensperger announces completion of voting machine audit using forensic techniques: No sign of foul play," (Nov. 17, 2020), available at https://sos.ga.gov/index.php/elections/secretary_raffensperger_announces_completion_of_voting_machine_audit_using_forensic_techniques_no_sign_of_foul_play.

[redacted]

11. [redacted]

12. Beyond demonstrating the feasibility of altering personal votes cast by individual voters on individual BMDs, the Curling Plaintiffs seek to prove that such an attack could be accomplished on a wide scale, depriving them and other Georgia

voters of their right to vote. There is a growing body of evidence that this is the case, beginning with Georgia's record of major election security lapses, such as the vulnerabilities at the Center for Election Systems discovered and exploited by Logan Lamb, the vulnerabilities in the online voter registration system that came to light on the eve of the 2018 general election, and the problems identified by Fortalice in the Secretary of State's computing infrastructure. Additional discovery is necessary to assess the full extent to which similar security gaps can facilitate wide-scale attacks on the BMDs.

13. [redacted]

14. [redacted]

15. [redacted]

[4] Dkt. 892-11.

16. The Curling Plaintiffs' technical investigations, as I understand the scope of my assignment in this case, are not intended to show that the outcome of any past election was maliciously altered. I understand that my assignment is not to analyze any specific election outcomes because the Curling Plaintiffs brought this case to protect their personal and individual right to vote, regardless of the outcome of any election, past or future. What my analyses demonstrate is that Curling Plaintiffs cannot be assured that the personal votes each of them casts on BMDs as individual voters will be counted correctly or perhaps at all. I expect that the further analyses I plan to conduct in this case, including with additional discovery, will further confirm this fact.

17. Unfortunately, the analysis I have conducted already shows that Georgia's new BMD equipment is even easier to compromise than the DRE equipment it replaced.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 12th day of February, 2021 in Rushland, Pennsylvania.

J. ALEX HALDERMAN